UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF MISSISSIPPI
ABERDEEN DIVISION

CRIS MARSH and **TAYLOR MARSH,** individually and on behalf of all others similarly situated, Plaintiffs, v. **CADENCE BANK,** Defendant.	Case No. 1:23-CV-136-SA-RP **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Cris Marsh and Taylor Marsh (collectively, "Plaintiffs") individually and on behalf of all others similarly situated (the "Class" or "Class Members"), bring this class action lawsuit against Defendant Cadence Bank ("Cadence" or "Defendant"). The following allegations are based on Plaintiffs' knowledge, investigations of counsel, facts of public record, and upon information and belief.

I. INTRODUCTION

1. Plaintiffs bring this class action lawsuit against Defendant for its failure to protect Plaintiffs' and the Class's highly sensitive Personally Identifiable Information ("PII"), including their names, addresses, dates of birth, Social Security numbers, driver's license numbers, and financial account information (such as credit card numbers, bank account numbers, and account statements) (collectively, the "Private Information" or "Personal Information"). As a result, well-known Russian cybergang Cl0p ("Clop") easily accessed

Defendant's servers, ***stealing*** the PII of Plaintiffs and the Class in a massive and preventable data breach (the "Data Breach" or "Breach"). Now, Plaintiffs' and the Class's confidential PII is in the hands of cybercriminals who have already posted it for sale on dark web and who have already begun to use it for nefarious purposes.

2. On June 1, 2023, Cadence learned that the file transfer application/software it used (the "Software"), and failed to adequately secure, was the subject of a cyberattack.

3. After the Breach, Cadence initiated an investigation and determined that cybercriminals "***accessed and downloaded***" the sensitive PII of Plaintiffs and the Class during the Data Breach.

4. Regrettably, Clop has already exploited the Private Information stolen in the Data Breach. Clop posted data obtained in the Breach on its dark web data leak site.[1]

5. None of this should have happened because the Data Breach was entirely preventable.

6. Indeed, Software users, such as Cadence, are each ***separately responsible*** for deciding what kinds of files to transfer using the Software, and for configuring the application to operate in a secure manner in their independent environments.

7. However, Cadence utterly failed to configure the Software to operate in a secure manner in its independent environment.

[1] *See* https://www.resecurity.com/blog/article/cl0p-ups-the-ante-with-massive-moveit-transfer-supply-chain-exploit.

8. On or around September 15, 2023, Cadence sent a letter titled "Notice of Data Breach" ("Notice Letter") to those impacted by the Data Breach, informing them that their Private Information was stolen in the Data Breach and was now at risk of misuse.

9. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves. Armed with the Private Information accessed in the Data Breach, data thieves can immediately commit a variety of sordid crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

10. Plaintiffs and the Class entrusted their Private Information to Cadence to receive financial services.

11. Defendant willingly accepted the responsibility to adequately secure, safeguard, protect, and maintain the PII of Plaintiffs and the Class.

12. There has been no assurance offered by Cadence that Cadence has adequately enhanced its data security practices within its own environment sufficiently to avoid a similar data breach in the future.

13. Similarly, Cadence has not stated it will terminate its use of the Software it failed to secure.

14. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

15. The improper access and theft of Plaintiffs' and Class Members' Private Information was a known risk to Defendants.

16. Specifically, Cadence knew that if it did not individually implement appropriate security measures with its use of the Software, that a data breach would occur and Plaintiffs' and the Class's PII would be unlawfully exposed and at risk.

17. Upon information and belief, Defendant failed to properly monitor its networks and systems, failed to properly implement adequate data security practices, procedures, infrastructure, and protocols, and failed to encrypt data. Had Defendant properly monitored and secured its computer digital environment, the Data Breach would not have happened.

18. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct as the Private Information that Defendant collected and maintained is now in the hands of data thieves and other unauthorized third parties. There is no question that well-known cybergang, Clop, has stolen Plaintiffs' and the Class's PII.

II. PARTIES

19. Plaintiff **Cris Marsh** (formerly known as Cris Fuentes) is, and at all times mentioned herein was, an individual citizen of Lewisville, Texas. Plaintiff Cris Marsh received

a Notice Letter from Defendant advising her that her PII was stolen in the Data Breach.[2]

20. Plaintiff **Taylor Marsh** is, and at all times mentioned herein was, an individual citizen of Lewisville, Texas. Plaintiff Taylor Marsh received a Notice Letter from Defendant advising him that his PII was stolen in the Data Breach.[3]

21. Defendant **Cadence Bank, N.A.** is a Mississippi based bank with approximately 413 branches across the states of Texas, Alabama, Mississippi, Arkansas, Missouri, Illinois, Louisiana, Tennessee, Georgia, Florida, and Oklahoma.[4] Cadence's principal place of business is located at 201 South Spring Street, Tupelo, Mississippi.

22. Class Members are domiciled across the United States.[5]

III. JURISDICTION AND VENUE

23. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and at least some members of the Class are citizens of states that differ from Defendant.

24. This Court has personal jurisdiction over Defendant because Defendant conducts a substantial amount of business in this District and is incorporated in the State of Mississippi.

---

[2] *See* Exhibit 1 (Notice Letter).

[3] *See* Exhibit 2 (Notice Letter).

[4] *See* https://cadencebank.com/find-a-location.

[5] *See* https://oag.ca.gov/ecrime/databreach/reports/sb24-573352 (California Attorney General Data Breach Notification); *see also* https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (Texas Attorney General Data Breach Notification).

25. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is in this District and many of Defendant's acts complained of herein occurred within this District.

IV. FACTUAL ALLEGATIONS

A. *Defendant's Businesses and the Collection of Plaintiffs' and Class Members' Private Information.*

26. Cadence Bank, established in 1876, is a Mississippi based bank that employs more than 6,479 people and generates approximately $1.8 billion in annual revenue. [6]

27. Cadence provides financial services to individuals and businesses across several states.[7]

28. To receive financial services from Cadence, Plaintiffs and the Class were required to provide Cadence with their PII.

29. Cadence used the Software to store and/or transfer Plaintiffs' and the Class's PII.

30. Because of the highly sensitive and personal nature of the information Cadence acquired and stored, Defendant promised to, among other things: keep Plaintiffs' and the Class's PII private; comply with industry standards related to data security; only use and release highly sensitive information stored for reasons that relate to the services they provide; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

---

[6] *See* https://www.jdsupra.com/legalnews/cadence-bank-confirms-moveit-data-5123726/.

[7] *See* https://cadencebank.com/.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that they each individually responsible for protecting Plaintiffs' and Class Members' Private Information to ensure it was not subject to unauthorized disclosure and exfiltration.

32. Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendant ultimately failed to do.

B. *The Data Breach and Defendant's Inadequate Notice to Plaintiffs and Class Members*

33. On June 1, 2023, Cadence learned that that the file transfer application it used, and failed to adequately secure, was infiltrated by cybercriminals in a massive and preventable data breach.

34. The Data Breach was perpetrated by the notorious cybergang, Clop, between May 28, 2023, through May 31, 2023.

35. During the Data Breach, cybercriminals had unfettered access to Plaintiffs' and the Class's PII.

36. Clop specifically took responsibility for the Data Breach on its data leak website on the dark web:[8]

[IMAGE ON NEXT PAGE]

[8] https://thecyberexpress.com/clop-leaks-victim-data-moveit-hack-clear-web/.

Screenshot of the names of victims posted by Clop (Photo: Dominic Alvieri/ Twitter)

37. Cadence admits that during the Data Breach, Plaintiffs' and the Class's PII was ***stolen*** by Clop. Specifically, Cadence stated that Clop "***accessed and downloaded***" highly sensitive PII such as: names, addresses, dates of birth, Social Security numbers, driver's license numbers, and financial account information (*e.g.*, credit card numbers, bank account numbers, and account statements).

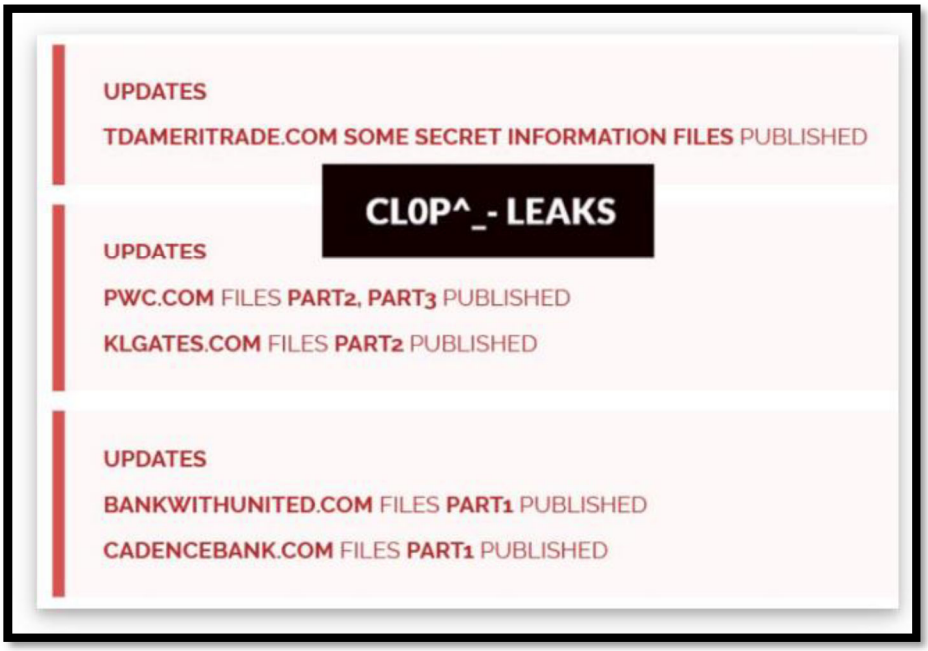
38. Thus, Clop accessed a cache of highly valuable Private Information through the Data Breach.

39. Cadence has yet to disclose how many individuals were impacted by the Data Breach.

40. Despite learning of the Data Breach on June 1, 2023, Cadence did not begin

notifying Data Breach victims that their PII had been exposed until on or around September 15, 2023 (the date of the Notice Letter). Thus, criminals were given over a three-month head start in misusing Plaintiff's and the Class's information.

41. Regrettably, Clop has already posted data it exfiltrated in the Data Breach on its dark web leak site:[9]



42. In fact, multiple websites have noted data obtained by Clop in the Cadence Breach is now on the dark web[10]:

[IMAGE ON NEXT PAGE]

[9] https://www.resecurity.com/blog/article/cl0p-ups-the-ante-with-massive-moveit-transfer-supply-chain-exploit.

[10] https://thecyberexpress.com/clop-leaks-victim-data-moveit-hack-clear-web/.

43. "[Clop] also threatened that the exfiltrated data will be posted on the clear web which will enable all the users to see the exposed data without using specialized tools that are required for dark web surfing."[11]

44. There is no question Plaintiffs' and the Class's PII was stolen in the Data Breach and is on the dark web.

45. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

46. Plaintiffs and Class Members provided their Private Information to Cadence

[11] *See* https://thecyberexpress.com/clop-leaks-victim-data-moveit-hack-clear-web/; *see also* https://www.resecurity.com/blog/article/cl0p-ups-the-ante-with-massive-moveit-transfer-supply-chain-exploit.

with the reasonable expectation and mutual understanding that Cadence would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

47. Plaintiffs and the Class also provided their PII to Cadence with the reasonable expectation and mutual understanding that Cadence would take appropriate measures to ensure the applications it used were secure.

48. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks in recent years, including recent similar attacks against secure file transfer companies like Accellion and Fortra carried out by the same Russian cybergang, Clop.[12]

49. Thus, Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

C. *Cadence has Independent Responsibility for the Data Breach and Could Have Prevented the Data Breach.* [13]

50. Cadence was independently responsible for securing its installation of the Software and could have prevented the Data Breach if it had taken this responsibility seriously.

---

[12] *See* https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware- gang/; *see also* https://www.bleepingcomputer .com/news/security/fortra-shares- findings-on-goanywhere-mft-zero-day-attacks/.

[13] At this time, Plaintiffs seek to hold *solely* Defendant Cadence Bank liable for the harms it inflicted upon Plaintiffs and the Class. Plaintiffs intentionally do not assert claims against Progress Software Corporation and/or Ipswitch and intentionally do not seek relief from Progress Software Corporation and/or Ipswitch. Plaintiffs allege Cadence Bank is separately and independently liable and responsible for the Data Breach.

51. Cadence has a network infrastructure specific to its organization and had the sole responsibility of designing and developing its security network.

52. It is up to Cadence to employ software and practices to control and monitor access to its data and systems.

53. Cadence was independently responsible for deciding what kinds of files to transfer using the Software and configuring the product to operate in a secure manner in its environments.

54. In sum, Cadence had the sole responsibility to determine:

a) How to protect and configure the environments in which the Software was operating;

b) What kind of data was transferred and stored via the Software;

c) Whether and how to encrypt that data; and

d) Whether to monitor or respond to early indicators that hackers were taking steps to access and exfiltrate that data.

55. The creator of the Software acknowledges as much and publishes detailed recommendations for users, such as Cadence, regarding the configuration of the Software:

> Updates, settings, accounts, and policies should be reviewed on a regular cadence to ensure the configuration is meeting current compliance frameworks and to review for unexpected activity or behavior that needs to be addressed. It is recommended that [the Software] administrators perform a regular security audit with their corporate security and compliance teams. Many teams perform this monthly or quarterly. This document is intended to provide [the Software] administrators with a starting point to create their own security checklist that can be used for regular reviews. The list is not exhaustive and not all recommendations will apply to all [Software]installations.[14]

[14] https://community.progress.com/s/article/MOVEit-Security-Best-Practices-Guide.

56. The creator of the Software gives a detailed installation and configuration manual so that the Software users are in control of the security features offered in the Software. Cadence disregarded these directives and failed to employ any security features in the Software.

57. The creator of the Software also provides an administrator guide and a security best practices guide to aid in configuring and securing the Software. However, Cadence disregarded these directives and did not implement them.

58. The Software is also dependent on other software such as Windows Server, Microsoft SQL Server (MSSQL) or MySQL, and IIS, which Cadence failed to secure.

59. Additionally, other software and hardware solutions are involved such as routers, firewalls, and mail servers which could have provided access to the Software server to those who should not have it, like Clop. Those other software solutions and systems are not produced or maintained by the creator of the Software and are not the responsibility of the creator of the Software to secure. It is the responsibility of Cadence, and Cadence did not take this responsibility seriously.

60. The data is hosted, maintained, and secured by Cadence, not the creator of the Software. Hence, Cadence did not secure the data it hosted and maintained.

61. Cadence was responsible for securing its installation of the Software and designing and securing the network infrastructure. However, Cadence utterly failed to do so.

62. This is evidenced by the fact that not all users of the Software were impacted.

63. Indeed, some of the Software users had appropriate monitoring and other security measures in place and, as a result, were able to detect and thwart efforts to exploit

the Software vulnerability on their systems.

64. For instance, on May 27, 2023, Akamai, a managed detection and response service that corporations can hire to monitor their data systems, detected the attack and prevented it. "Akamai researchers detected exploitation attempts against one of Akamai's financial customers — an attack that was blocked by the Akamai Adaptive Security Engine."[15]

65. For this particular vulnerability with the Software, Cadence exercising some basic security practices would have mitigated the vulnerability, to gain access, which would have prevented the Breach.

66. Clop used the ATT&CK Techniques for Enterprise.

67. Clop simply exploited a weakness the Software to write a file to the web server which was a Remote Access Tool.

68. Security measures to prevent unauthenticated users from Russian IP addresses accessing the server would have stopped the Breach in its tracks. However, Cadence did not have these security measures in place.

69. A deny all default approach to security would have prevented the Breach. However, Cadence did not have this in place.

70. Any one of the following security measures, if employed by Cadence, could have stopped the Data Breach from occurring:

a) **Denying write access to all but local account used for writing to the web directory.** There is no reason to grant unauthenticated user access and all user access to a file or directory that does not

[15] *See* https://www.akamai.com/blog/security-research/moveit-sqli-zero-day-exploit-clop-ransomware.

need write access. Additionally, there are solutions with the Software and third-party solutions to provide an email or SMS notification in the event files are accessed, created, or modified.

b) **A firewall dropping all packets originating from IP addresses outside of the organization.** By dropping all packets from foreign IP addresses, this would have prevented Clop the ability to connect to perform the SQL injection.

c) **Placing the server in a DMZ.** This would have prevented Clop from delivering the TrueBot malware stopping the Data Breach. Publicly facing web servers can provide an attacker access inside the organization where they can traverse systems on the inside of any perimeter firewalls. A DMZ would help mitigate that vulnerability.

71. Unfortunately for Plaintiffs and the Class, Cadence failed to implement any of the above measures prior to the Data Breach resulting in serious demonstrable harm.

D. *Cadence Failed to Comply with FTC Guidelines*

72. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

73. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored

on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

74. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers, have implemented reasonable security measures.

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

76. As evidenced by the Data Breach, Cadence failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

77. Defendant was at all times fully aware of its obligations to protect the Private Information of Plaintiffs and Class Members yet failed to comply with such obligations.

Defendant was also aware of the significant repercussions that would result from its failure to do so.

78. Banks and other financial companies are routinely identified as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.[16]

79. Some industry best practices that should be implemented by businesses like Defendant include but are not limited to educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Cadence failed to follow some or all these industry best practices.

80. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff and customers regarding these points. As evidenced by the Data Breach, Cadence failed to follow these cybersecurity best practices.

81. Cadence failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-

[16] *See* https://www.cfo.com/news/financial-industry-is-third-most-targeted-by-hackers/654808/; https://www.comparitech.com/blog/vpn-privacy/financial-data-breaches/.

5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

82. Cadence failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. *Cadence Breached its Duties to Safeguard Plaintiffs' and Class Members' Private Information.*

83. In addition to their obligations under federal and state laws, Cadence owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, transferring, storing, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

84. Cadence owed a duty to Plaintiffs and Class Members to provide reasonable data security, including complying with industry standards and requirements, training for its staff, and ensuring that its computer systems, software, networks, and protocols adequately protected the Private Information of Class Members.

85. Defendant breached its duties and obligations owed to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard Plaintiffs' and the Class's PII. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. failing to adequately protect customers' Private Information;

c. failing to properly monitor its own data security systems for existing intrusions;

d. failing to properly oversee and monitor the Software;

e. failing to sufficiently train its employees regarding the proper handling of its customers' files containing the Private Information;

f. failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

g. failing to adhere to industry standards for cybersecurity as discussed above; and

h. otherwise breaching duties and obligations to protect Plaintiffs' and Class Members' Private Information.

86. Cadence negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing Clop to easily access its systems, and servers which contained unsecured and unencrypted Private Information.

87. Had Cadence remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems through the Software, and ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

88. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendant.

F. *Defendant Should Have Known that Cybercriminals Target PII to Carry Out Fraud and Identity Theft*

89. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[17]

90. Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment.

91. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

92. Indeed, Clop has already extorted Cadence and posted data obtained in the Breach on the dark web.[18]

93. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and

---

[17] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff- perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

[18] https://thecyberexpress.com/clop-leaks-victim-data-moveit-hack-clear-web/.

date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

94. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

95. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

96. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts,

placing a freeze on their credit, and correcting their credit reports.[19] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

97. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

98. PII can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

99. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[20] The increase in

---

[19] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps.

[20] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr announces-indictment-fourmembers-china-s-military.

cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

100. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[21] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[22]

101. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[23]

---

[21] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[22] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the- dark-web/.

[23] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/.

102. The Dark Web Price Index of 2022, published by PrivacyAffairs[24] shows how valuable just email addresses alone can be, even when not associated with a financial account:

Email Database Dumps	Avg. Price USD (2022)
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

103. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

104. Likewise, the value of PII is increasingly evident in our digital economy. Many companies collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and shares it with third parties for similar purposes.[25]

105. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[26]

106. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at

---

[24] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/.

[25] *See* https://robinhood.com/us/en/support/articles/privacy-policy/.

[26] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

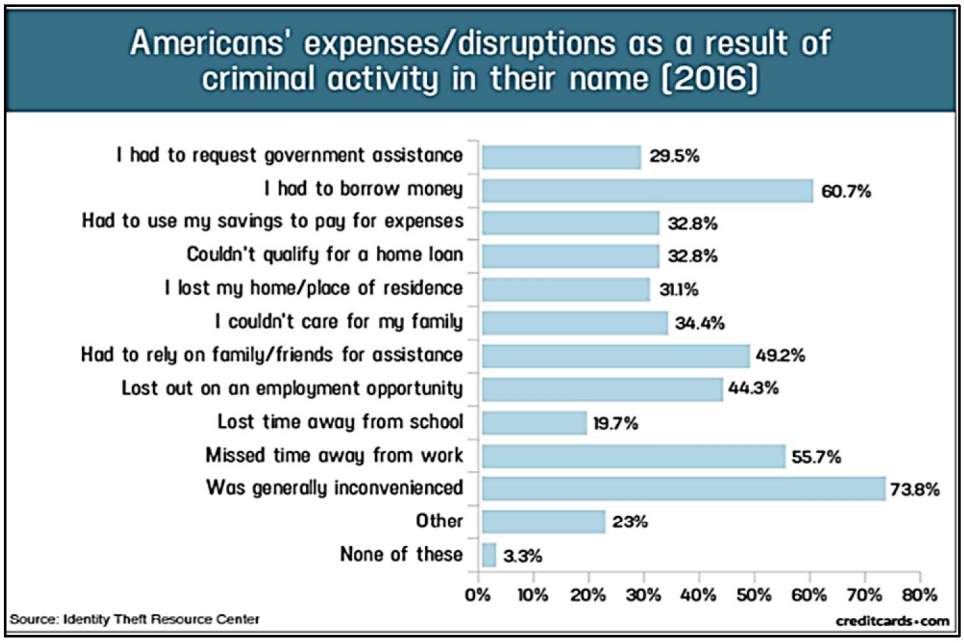
107. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

108. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace.

109. A study by the Identity Theft Resource Center[27] shows the multitude of harms caused by fraudulent use of PII:

[IMAGE ON NEXT PAGE]

[27] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (image no longer available).



110. It must also be noted that there ***may*** be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[28]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

111. PII is such a valuable commodity to identity thieves that once the information

[28] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html.

has been compromised, criminals often trade the information on the "cyber black market" for years.

112. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. *Plaintiffs' Individual Experiences*

Plaintiff Taylor Marsh

113. Plaintiff Taylor Marsh provided his PII, including his name, address, date of birth, Social Security number, driver's license number, and financial account information (such as credit card numbers, bank account numbers, and account statements) to Cadence in connection with a mortgage loan application prior to the Data Breach.

114. On or around September 15, 2023, Plaintiff Taylor Marsh received a Notice Letter from Cadence notifying him that his name, address, date of birth, Social Security number, driver's license number, and financial account information (such as credit card numbers, bank account numbers, and account statements) were "***accessed and downloaded***" in the Data Breach.[29]

115. The PII Cadence failed to protect and that was subsequently exfiltrated by cybercriminals has already been misused for nefarious purposes following the Data Breach.

116. Specifically, after the Data Breach, Plaintiff experienced the following fraud and identity theft:

a) An unknown fraudulent actor opened a checking account and a savings account

[29] *See* Exhibit 2.

in his name through Regions Bank. When he attempted to close the accounts, he was initially unable to because the accounts were being actively used by the fraudulent actor.

b) Multiple unauthorized fraudulent hard inquiries on his credit report through institutions such as Fairwinds Credit Union, Ally Financial, Comenity Capital Bank (Alphaeon-Opthamology), Mercedes Benz, JPMCB Auto Finance, Lightstream, Bank of America, Carmax, and Jared.

c) Multiple unauthorized and fraudulent attempts to open credit cards under his name;

d) Multiple unauthorized and fraudulent attempts to obtain car loans in his name, including attempts through Ally Bank, Bank of America, and Truist; and

e) A fraudulent auto policy was obtained under his name.

117. After the Data Breach, Plaintiff Taylor Marsh filed a police report reporting he was a victim of identity theft and fraud.

118. Plaintiff Taylor Marsh reasonably believes the actual misuse he has experienced following the Data Breach is a direct result of his PII being stolen in the Data Breach. Specifically because the PII that was stolen in the Data Breach is the same types of PII needed to commit the actual misuse described above.

119. As a direct and traceable result of the Data Breach, Plaintiff Taylor Marsh estimates he has spent ***at least 35 hours*** researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, reviewing credit reports for fraudulent activity, and mitigating the fraud and identity theft that has already occurred. However, this

is not the end. Plaintiffs and the Class will now be forced to expend additional time to review their credit reports and monitor their accounts for the rest of their lives. This is time spent at Defendant's direction, which has been lost forever and cannot be recaptured.

120. Plaintiff Taylor Marsh places significant value in the security of his PII and does not readily disclose it. Plaintiff Taylor Marsh entrusted his PII to Defendant with the understanding that Defendant would keep his information secure and that Defendant would employ reasonable and adequate security measures to ensure that his PII would not be compromised.

121. As a direct and traceable result of the Data Breach, Plaintiff Taylor Marsh suffered actual damages such as: (i) theft of his PII; (ii) fraud and identity theft; (iii) lost time related to monitoring his accounts for fraudulent activity and mitigating the fraud and identity theft he has already experienced; (iv) loss of privacy due to his PII being exfiltrated by cybercriminals and published on the dark web; (v) loss of the benefit of the bargain because Defendant did not adequately protect his PII; (vi) severe emotional distress because identity thieves now possess his PII; (vii) exposure to an increased and imminent risk of fraud and identity theft now that his PII has been stolen and misused; (viii) loss in value of his PII due to her PII being in the hands of cybercriminals who can use it at their leisure; and (ix) other economic and non-economic harm.

122. As a direct and traceable result of the Data Breach, Plaintiff Taylor Marsh has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for ***years*** to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach

and the fact that extensive misuse has already occurred.

123. Cadence acknowledged the increased risk of future harm Plaintiffs and the Class now face by offering complimentary credit monitoring services to Plaintiffs and the Class. Such an offer was woefully inadequate as it will not prevent identity theft and fraud but will only alert Plaintiffs once it has already occurred. Cadence's measly two (2) year offering of services completely ignores the fact that Plaintiffs and the Class will be at a significant and imminent risk of future harm for the rest of their lives.

124. Knowing that thieves intentionally targeted and stole his PII, including his Social Security number and financial information, knowing that Clop has already released data obtained in the Breach on the dark web, and having already experienced identity theft and fraud has caused Plaintiff Taylor Marsh great anxiety beyond mere worry. Specifically, Plaintiff Taylor Marsh has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that his PII has been stolen and misused as a result of the Data Breach.

125. Plaintiff Taylor Marsh has a continuing interest in ensuring that his PII which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

126. As a direct and traceable result of the Data Breach, Plaintiff Taylor Marsh will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come and will have to pay an identity monitoring company for the rest of his life to protect his PII.

Plaintiff Cris Marsh

127. Plaintiff Cris Marsh provided her PII, including her name, address, date of birth, Social Security number, driver's license number, and financial account information (such as credit card numbers, bank account numbers, and account statements) to Cadence in connection with a mortgage loan application prior to the Data Breach.

128. On or around September 15, 2023, Plaintiff Cris Marsh received a Notice Letter from Cadence notifying her that her name, address, date of birth, Social Security number, driver's license number, and financial account information (such as credit card numbers, bank account numbers, and account statements) were "***accessed and downloaded***" in the Data Breach.[30]

129. As a direct and traceable result of the Data Breach, Plaintiff Cris Marsh estimates she has spent ***approximately 15 hours*** researching the Data Breach, reviewing and monitoring her accounts for fraudulent activity, and reviewing credit reports for fraudulent activity. However, this is not the end. Plaintiffs and the Class will now be forced to expend additional time to review their credit reports and monitor their accounts for the rest of their lives. This is time spent at Defendant's direction, which has been lost forever and cannot be recaptured.

130. Plaintiff Cris Marsh places significant value in the security of her PII and does not readily disclose it. Plaintiff Cris Marsh entrusted her PII to Defendant with the understanding that Defendant would keep her information secure and that Defendant would employ reasonable and adequate security measures to ensure that her PII would not be

[30] *See* Exhibit 1.

compromised.

131. As a direct and traceable result of the Data Breach, Plaintiff Cris Marsh suffered actual damages such as: (i) theft of her PII; (ii) lost time related to monitoring her accounts for fraudulent activity; (iii) loss of privacy due to her PII being exfiltrated by cybercriminals and published on the dark web; (iv) loss of the benefit of the bargain because Defendant did not adequately protect her PII; (v) severe emotional distress because identity thieves now possess her PII; (vi) exposure to an increased and imminent risk of fraud and identity theft now that her PII has been stolen; (vii) loss in value of her PII due to her PII being in the hands of cybercriminals who can use it at their leisure; and (viii) other economic and non-economic harm.

132. As a direct and traceable result of the Data Breach, Plaintiff Cris Marsh has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for ***years*** to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach, the fact that Plaintiff Taylor Marsh has already experienced misuse, and the fact that cybercriminals have admitted to stealing it and posting data obtained in the Breach on the dark web.

133. Cadence acknowledged the increased risk of future harm Plaintiffs and the Class now face by offering complimentary credit monitoring services to Plaintiffs and the Class. Such an offer was woefully inadequate as it will not prevent identity theft and fraud but will only alert Plaintiffs once it has already occurred. Cadence's measly two (2) year offering of services completely ignores the fact that Plaintiffs and the Class will be at a

significant and imminent risk of future harm for the rest of their lives.

134. Knowing that thieves intentionally targeted and stole her PII, including her Social Security number and financial information, knowing that Clop has already released data obtained in the Breach on the dark web, and having already experienced identity theft and fraud has caused Plaintiff Cris Marsh great anxiety beyond mere worry. Specifically, Plaintiff Cris Marsh has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that her PII has been stolen as a result of the Data Breach.

135. Plaintiff Cris Marsh has a continuing interest in ensuring that her PII which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

136. As a direct and traceable result of the Data Breach, Plaintiff Cris Marsh will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come and will have to pay an identity monitoring company for the rest of her life to protect her PII.

H. *Plaintiffs' and Class Members' Damages*

137. Plaintiffs and Class Members would not have provided their PII to Cadence had Cadence disclosed it lacked adequate data security.

138. Additionally, Plaintiffs and Class Members would not have permitted their PII to be transmitted and/or stored via the Software had Cadence disclosed it took no measures to secure it.

139. Plaintiffs and Class Members have suffered actual injury in the form of time

spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach.

140. Plaintiffs and Class Members suffered actual injury in the form of having their Private Information stolen and published on the dark web as a result of the Data Breach.

141. Plaintiffs and Class Members suffered actual injury in the form of damages to and diminution in the value of their Private Information – a form of intangible property that Plaintiffs and Class Members entrusted to Cadence.

142. Plaintiffs and Class Members suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

143. Plaintiffs and the Class have a continuing interest in ensuring that their Private Information, which remains in Defendant's possession and stored within the Software, is protected, and safeguarded from future breaches.

144. Plaintiffs and Class Members also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of their Private Information, a form of property that Defendant obtained from them; (b) violation of their privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud they now face.

145. As a result of the Data Breach, Plaintiffs and many Class Members anticipate spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

146. In sum, Plaintiffs and Class Members have been damaged by the compromise

of their Private Information in the Data Breach.

147. Plaintiffs' and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Cadence's failure to ensure it employed adequate data security with the use of the Software.

148. As a direct and proximate result of Defendant's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of fraud and identity theft.

149. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

150. The Private Information maintained by and stolen from Defendant, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

151. Additionally, as a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and/or closely reviewing and monitoring bank accounts and

credit reports for unauthorized activity for years to come.

152. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

153. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was accessed, viewed, and acquired by Clop in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists.[31] In 2019, the data brokering industry was worth roughly $200 billion. In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker who in turn aggregates the information and provides it to other companies.[32] Consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[33]

154. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for

---

[31] *See* Data Coup, https://datacoup.com/.

[32] *What is digi.me?, DIGI.ME,* https://digi.me/what-is-digime/.

[33] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

155. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Addressing their inability to withdraw funds linked to compromised accounts;

d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

e. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

f. Contacting financial institutions and closing or modifying financial accounts;

g. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

h. Paying late fees and declined payment fees imposed as a result of

failed automatic payments that were tied to compromised cards that had to be cancelled; and

i. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

156. Moreover, Plaintiffs and Class Members have a continuing interest in ensuring that their Private Information, which is believed to still be in the possession of Defendants, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password- protected, and that such data is properly encrypted.

157. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

158. Plaintiffs brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23.

159. Specifically, Plaintiffs proposes the following Nationwide Class (referred to herein as the "Class" or "Class Members"), subject to amendment as appropriate:

Nationwide Class

All individuals who reside in the United States who received a Notice of Data Breach Letter from Defendant.

160. Excluded from the Class is Defendant and its parents or subsidiaries, any

entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

161. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class, as well as add subclasses, before the Court determines whether certification is appropriate.

162. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23.

163. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class likely consists of thousands of individuals whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Defendants' records.

164. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Cadence engaged in the conduct alleged herein;

b. When Cadence learned of the Data Breach;

c. Whether Cadence's response to the Data Breach was adequate;

d. Whether Cadence unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

e. Whether Cadence failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether Cadence failed to employ appropriate data security measures within the Software;

g. Whether Cadence failed to oversee and monitor the Software;

h. Whether Cadence's data security practices related to the Software prior to and during the Data Breach complied with applicable data security laws and regulations;

i. Whether Cadence owed a duty to Class Members to safeguard their Private Information;

j. Whether Cadence breached it duties to Class Members to safeguard their Private Information;

k. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

l. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

m. Whether Cadence knew or should have known that its data security systems and monitoring processes as it relates to the Software were deficient;

n. What damages Plaintiffs and Class Members suffered as a result of Defendant's misconduct;

o. Whether Defendant's conduct was negligent;

p. Whether Defendant's conduct was *per se* negligent;

q. Whether Defendant breached an implied contract with Plaintiffs and Class Members:

r. Whether Defendant's were unjustly enriched;

s. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiffs and Class Members are entitled to credit or identity monitoring and monetary relief; and

u. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

165. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

166. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

167. Predominance. Cadence has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above

predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

168. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for PSC. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

169. Class certification is also appropriate. Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

170. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names, addresses, and/or email addresses of Class Members affected by the Data Breach.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE

171. Plaintiffs restate and reallege the allegations stated above as if fully set forth herein.

172. Cadence knowingly collected, acquired, and stored Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

173. To fulfill this duty of care, Cadence was required to ensure it maintained adequate data security, procedures, systems, infrastructure, and protocols and implemented such across its entire network environment.

174. Cadence was also required to oversee, monitor, and adequately protect all software it utilized to store and transfer Plaintiffs' and the Class's PII.

175. Cadence's duty also included a responsibility to implement processes by which it could detect and analyze a vulnerability quickly and to give prompt notice to those affected in the case of a cyberattack.

176. Cadence knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate data security.

177. Cadence was on notice because, on information and belief, it knew or should have known of the substantial increase in cyberattacks in recent years, including recent similar

attacks against Accellion and Fortra carried out by the same Russian cyber gang, Clop.

178. After all, Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, transferring, and storing the Private Information of Plaintiffs and Class Members. Thus, Defendant knew, or should have known, the importance of exercising reasonable care in handling the Private Information entrusted to it.

179. Cadence owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems, software, and networks, and the personnel responsible for them, adequately protected the Private Information in its possession.

180. Cadence breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. And but for Cadence's negligence, Plaintiff and Class Members would not have been injured. The specific negligent acts and omissions committed by NEG include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to employ adequate security measures in its use of the Software;

c. Failing to comply with —and thus violating— the Federal Trade Commission Act and its rules and regulations;

d. Failing to adequately monitor the security of its networks, systems, and software;

e. Failing to ensure that the Software had security in place to maintain reasonable data security safeguards;

f. Failing to have in place mitigation policies and procedures;

g. Allowing unauthorized access to Class Members' Private Information;

h. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

i. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

181. Under the Federal Trade Commission Act and the FTC's rules and regulations, Defendant had a duty to employ reasonable security measures. Specifically, this statute prohibits "unfair . . . practices in or affecting commerce," including (as interpreted and enforced by the FTC) the unfair practice of failing to use reasonable measures to protect confidential data. Plaintiffs and the Class are precisely the class of individuals the FTCA was designed to protect.

182. Moreover, Plaintiffs and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that Defendant inflicted upon Plaintiffs and Class Members.

183. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant

are bound by industry standards to protect confidential Private Information.

184. Defendant owed Plaintiffs and members of the Class a duty to notify them within a reasonable time frame of any breach of their Private Information. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiffs and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of Defendant's Data Breach.

185. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Defendant actively sought and obtained the Private Information of Plaintiffs and Class Members.

186. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial industry. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

187. Simply put, Defendant's negligence actually and proximately caused Plaintiffs and Class Members' actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their Private Information by criminals, improper

disclosure of their Private Information, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence. Moreover, injuries-in-fact and damages are ongoing, imminent, and immediate.

188. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

189. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (1) strengthen its data security systems and monitoring procedures regarding the Software; (2) submit to future annual audits of those systems and monitoring procedures; and (3) to provide adequate credit monitoring to all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT

190. Plaintiffs restate and reallege the allegations stated above as if fully set forth herein.

191. Plaintiffs and the Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect their Private Information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

192. Plaintiff and the Class were required to, and delivered, their Private Information to Defendant as part of the process of obtaining financial services.

193. Plaintiffs and Class Members conferred a monetary benefit on Defendant in that Plaintiffs paid money to Defendant in exchange for services. Part of this monetary benefit

was to be used to provide a reasonable level of data security to protect Plaintiffs' and the Class's Private Information.

194. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services.

195. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under state and federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

196. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

197. Based on the implicit understanding, Plaintiff and Class Members accepted Defendant's offers for services and provided Defendant with their Private Information.

198. Plaintiff and Class Members would not have permitted their Private Information to be collected and stored by Defendant had they known that Defendant would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

199. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

200. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

201. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Cadence's breach of its implied contracts with Plaintiff and Class members.

202. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

203. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (1) strengthen its data security systems and monitoring procedures regarding the Software; (2) submit to future annual audits of those systems and monitoring procedures; and (3) to provide adequate credit monitoring to all Class Members.

COUNT III
UNJUST ENRICHMENT

204. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

205. This Count is pleaded in the alternative to Counts I and II.

206. Plaintiffs and Class Members conferred a benefit on Defendant by surrendering their Private Information to Cadence.

207. Cadence derived profits from Plaintiffs and the Class's PII because it allowed them to provide services and derive revenue therefrom.

208. As such, a portion of the payments made to Cadence, which payments would not be possible without Plaintiffs and Class Members turning over their Private Information, was to be used to provide a reasonable and adequate level of data security that was in compliance with applicable state and federal regulations and industry standards. However, Cadence did not do this. Rather, Cadence retained the benefits of its unlawful conduct, including the amounts of payment received that should have been used for adequate cybersecurity practices that it failed to provide.

209. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it, which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures, which would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

210. If Plaintiffs and Class Members had known that Defendant would not adequately secure their Private Information, they would not have agreed to provide such Private Information.

211. Due to Defendant's conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendant to be permitted to retain the benefits of their wrongful conduct.

212. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and/or are at a substantial and continuous risk of suffering injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and theft of their

Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

213. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

214. Plaintiffs and Class Members plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Federal Rule of Civil Procedure 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class, including but not limited to requirements that Defendant (1) strengthen its data security systems and monitoring procedures regarding the Software; (2) submit to future annual audits of those systems and monitoring procedures; (3) provide adequate lifetime credit monitoring and identity theft insurance to all Plaintiffs and Class Members; and, if appropriate, provide for a constructive trust.

d. An order requiring Defendant to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees,

costs, and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: October 12, 2023

s/ Robert B. McDuff
Law Office of Robert McDuff
767 North Congress Street
Jackson, MS 39202
Telephone: (601) 259-8484
rbm@mcdufflaw.com

William B. Federman*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com

Pro hac vice application forthcoming

Counsel for Plaintiffs